CONSOLIDATED INFORMATION TECHNOLOGY SERVICES
TASK ASSIGNMENT (TA)

1. **TITLE:** (B703) General Support for the Center IT Security Manager

TA No:	SLC001-Rev14		
Task Area Monitor:		**Alternate Task Area Monitor:**	
NASA POC:		**Software Control Class:**	Low Control
Type of Task:	Recurring Task		

2. BACKGROUND

This revision covers additions/revisions pertaining to ITS technology evaluation, security license acquisition, firewall monitoring, and patch management.

This area of work is in support of the LaRC Information Technology (IT) Security Manager (ITSM) or Designee to implement the IT Security (ITS) Program at LaRC in accordance with NPR 2810.1A, Security of Information Technology (see the following URL: http://nodis.hq.nasa.gov).

This Task assignment includes:
1. System Compliance and Vulnerability Reduction
2. Perimeter Protection for LaRCNET
3. Incident Response and Computer Forensics
4. Intrusion Detection and Monitoring
5. Outreach
6. IT Security Helpdesk
7. Certification and Accreditation

3. OBJECTIVE

The objective of this TA is to provide NASA Langley Research Center with an incident response and computer forensics capability; intrusion detection and monitoring capability; remote access and network access control capability; internet filtering and penetration testing; support of IT system security plans; coordination of ITS activities with other Centers; perimeter protection, to include a Virtual Private Network (VPN) and firewall; and outreach. This TA also provides system administration support for the IT Security server and tool systems listed on Exhibit A of this TA including the Langley Registration Authority (RA) for the NASA LaRC Public Key Infrastructure (PKI) at NASA LaRC as part of the IT Security initiative.

4. GENERAL IT SUPPORT SERVICES

Services Specified Through Exhibit A:

Refer to Exhibit A, Inventory of Equipment and Software (attached), that has been completed to define the required general IT support services for intrusion detection and monitoring, perimeter protection for LaRCNET, penetration testing, and the Langley RA for the NASA PKI.

The level of security shall be consistent with National Aeronautics and Space Administration (NASA) procedures and directives and in accordance with National Institute of Standards and Technology (NIST) guidelines.

Any system software, application software, or database software that is licensed to run on a particular item of equipment is entered in the respective column for that item. Software that does not require a license is also included if it is relevant to any of the required services.

The services of System Administration (SA), Hardware Maintenance (HM), System Software Maintenance (SSM), Applications Management (AM), and Database Administration (DBA), are required for the items of equipment or software that are checked in the respective columns of Exhibit A.

Maintenance of Software Developed By or For LaRC:
Scripts, applications and other tools developed locally by the contractor IT Security team to enhance the efficiency, productivity or usefulness of a system or COTS package(s) will be documented internally (describing the functions) and externally (describing the use). This documentation will be stored for easy access. The contractor will ensure multiple personnel are familiar with the operation of all scripts, applications and tools.

The contractor is responsible for maintaining current licenses for systems under the Exhibit A attached.

The contractor IT security team is responsible for maintaining the confidentiality, integrity and availability of any data collected or generated for use by LaRC IT security, within the bounds of the government's systems and data stores available.

General IT Support Services Performance Metrics

Performance Standard: The contractor shall prepare a report of the impact of any incident to include costs due to the loss of data; time lost due to the unavailability of the system; time to rebuild the system; time to investigate the incident; and any other factors with a cost implication. The report shall also include findings on the method of intrusion and corrective actions taken to reduce the system's vulnerability. This report is due one week after local investigation is completed.

Performance Metrics:

Exceeds: Delivery exceeds schedule with proactive solutions included in the report.

Meets: Delivery schedule met with no or only minor revisions to the report.

Fails: Late delivery and/or inadequacies in the report.

Performance Standard: Perform incident response and computer forensics investigations at the request of the NASA Center ITSM or representatives.

Performance Metrics:

Exceeds: Performs the investigation without loss of evidence and reports to the

Center ITSM as appropriate during the investigation, and provides recommendations as to improvements in the process.

Meets: Performs the investigation with minimal loss of evidence and reports to the Center ITSM as appropriate during the investigation.

Fails: Report is late or significant loss of data occurs due to the contractors actions.

Performance Standard: Notification of Center ITSM or his/her designee of a suspected incident within one hour of discovery during the hours of 8:00AM to 5:00PM, Monday-Friday, or via secure e-mail at all other times. The contractor shall notify the Agency Security Operations Center (SOC) and the OIG within two hours of the initial report to the Center ITSM of a suspected incident, unless it is determined that no incident occurred within the first two hours. Notification of suspected incidents shall be made through direct face-to-face contact, via telephone or by secure e-mail.

Performance Metrics:

Exceeds: Notification is usually faster than two hours with proactive responses in progress.

Meets: Notification is rarely delayed beyond two hours; timely proactive responses.

Fails: Notification is frequently longer than two hours; proactive responses are delayed.

Performance Standard: The Contractor shall support the Center ITSM through coordination of ITS activities with ITS personnel at other NASA Centers and the SOC.

Performance Metrics:

Exceeds: Multiple contract personnel are usually in attendance at local telephone or video conferences. Deliverables for working groups or the SOC meet schedules and receive good reviews.

Meets: At least one contract person is in attendance at every telephone or video conference. Deliverables for working groups or the SOC meet schedules with only minor delays.

Fails: Contract personnel frequently miss local telephone or video conferences. Deliverables for working groups or the SOC have major delays.

Performance Standard: A monthly report on intrusion detection and monitoring, hostile scans and other attacks on LaRCNET (i.e., perimeter protection) is given to the Center ITSM within 5 working days after the end of each month.

Performance Metrics:

Exceeds: The contractor will provide the Center ITSM a monthly report no more than 2 business days after the end of each month.

Meets: The contractor will provide the Center ITSM a monthly report no more than 5 business days after the end of each month.

Fails: The contractor will provide the Center ITSM a monthly report more than 5 business days after the end of each month.

Performance Standard: The LaRC ITS web-site is maintained.

Performance Metrics:

Exceeds: The site is maintained in an up-to-date manner, with modifications made within 3 days of being requested. There are no discrepancies with compliance to Federal, NASA or LaRC regulations or policies

Meets: The site is almost always up-to-date. Modifications are made within 5 days of being requested. There are only minor discrepancies with compliance to Federal, NASA or LaRC regulations or policies

Fails: The site is frequently out-of-date or not in compliance with Federal, NASA or LaRC regulations or policies. Modifications are not made within 5 days of being requested.

Performance Standard: The help desk function will be available from 8:00 a.m. untill 5:00 p.m. Monday through Friday. A report will be generated monthly detailing the number of calls, and topics (by category) that were requested.

Performance Metrics:

Exceeds: Delivery exceeds schedule and/or contains suggestions for improvement in efficiency included in the report.

Meets: Delivery schedule met with no or only minor revisions to the report.

Fails: Late delivery and/or inadequacies in the report.

Performance Standard: Report on vulnerability reduction as scheduled and directed by the Center ITSM.

Performance Metrics:

Exceeds: Reporting meets the schedule and innovative measures are utilized to ensure the continuing reduction of vulnerabilities.

Meets: Reporting is sometimes late.

Fails: Reports usually fail to meet the schedule and no follow-on work is performed to ensure the continuing reduction of vulnerabilities.

Performance Standard: Maintain a secure web-site to post the results of periodic scans on an organization-by-organization basis to facilitate response by the appropriate system administrators.

Performance Metrics:

Exceeds: The site is maintained in an up-to-date manner. Scan results are posted within one week of being requested. There are no discrepancies with compliance to Federal, NASA or LaRC regulations or policies.

Meets: The site is almost always up-to-date. Scan results are posted within two weeks of being requested. There are only minor discrepancies with compliance to Federal, NASA or LaRC regulations or policies.

Fails: The site is frequently out-of-date or not in compliance with Federal, NASA or LaRC regulations or policies.

Performance Standard: Re-establish connectivity to the Internet after a failure of either the Center firewall or VPN. The particular circumstances of a failure will be considered in evaluating performance.

Performance Metrics:

Exceeds: After notification of a failure: During normal duty hours, connectivity is restored in less than one hour.

Meets: After notification of a failure: During normal duty hours, connectivity is restored in less than three hours.

Fails: After notification of a failure: During normal duty hours, connectivity is frequently not restored in less than eight hours.

5. SYSTEM AND APPLICATION DEVELOPMENT SERVICES

None required.

6. WORK-AREA SPECIFIC SERVICES

Work Area Title: Incident Response and Computer Forensics

LaRC Manager: Center IT Security

Work Area Description: NASA Langley Research Center and nearby Contractor facilities with connections to LaRCNET.

Work Area Requirements: The Contractor shall maintain a trained Incident Response Team to support the Center ITSM in the Center's response to suspect ITS incidents. At the direction of the Center ITSM, the involved Contractor ITS staff will work with the Office of the Inspector General (OIG); affected data owners; system administrators; the ODIN Contractor: the NASA Incident Response Team and other entities. Notification of a suspected incident to the Center ITSM shall be done within one hour during normal working hours (8:00 a.m. Eastern Time until 5:00 p.m. Eastern Time Monday through Friday). If the Center ITSM is not available, either the Deputy Center ITSM, Center IT Security Technical Lead, Head of the IT Infrastructure Branch (ITIB), Assistant Head of ITIB, Center CIO, or Deputy CIO shall be notified within the same time period. Outside normal working hours, notification shall be by 9:00 a.m. the next business day. If no one is available, the Contractor shall take steps to notify the SOC and the OIG in the name of the Center ITSM. With concurrence of the Center ITSM, the Contractor shall implement tools and procedures for alerting appropriate personnel of security incidents on a near-real time basis. The Contractor shall take prudent steps to protect critical IT resources and information in the absence of any direct involvement by the Center ITSM or his designees.

All Contractor ITS staff are assigned to the Incident Response Team, although not everyone will have a role in every incident. Members of the Incident Response Team may have other assigned duties; however, those will not interfere with response to any incident. Team members shall have a mix of knowledge about the operating systems in use at LaRC, to include but not be limited to Macintosh, Microsoft Windows, Solaris, IRIX, AIX, LINUX, and other UNIX operating systems. Team members shall be able to utilize ITS software tools to analyze system logs to determine if there is a suspected incident. Once a potential incident is identified, the first priority is containment to limit the number of affected LaRC systems and data. The Contractor will also recommend corrective actions necessary to repair the damage and return the system to an operational status. Also the Contractor will recommend preventative measures of IT Security incidents.

Work Area Title: Outreach

LaRC Manager: Center IT Security

Work Area Description: NASA Langley Research Center and other NASA Centers.

Work Area Requirements: The Contractor shall conduct training and develop hands-on exercises for topics as directed by the Center ITSM to improve the understanding of Langley personnel of the importance of ITS as well as specific advice to assist them to secure systems. The Contractor shall also maintain an e-mail alias or aliases to facilitate the distribution of the SOC and Intellishield bulletins, virus warnings and messages from the Center ITSM to the appropriate Langley personnel.

The Contractor shall support the Center ITSM through coordination of ITS activities with ITS personnel at other NASA Centers and the SOC by:
-Attend, on an as needed basis, weekly or special phone or video conferences to discuss ITS issues.
-Input to the SOC or the NCC-ITS as required by other tasks or the Center ITSM.
-Support for ITS services in conjunction with the Lockheed-Martin (LMIT) Help Desk for Langley personnel.

Work Area Title: Intrusion Detection and Monitoring

LaRC Manager: Center IT Security

Work Area Description: NASA Langley Research Center - Building 1268 complex and other facilities with connections to LaRCNET as required.

Work Area Requirements: The intrusion detection and monitoring capabilities shall be operational seven days per week, 24 hours per day . The Contractor shall operate and monitor both the hardware and software that comprise the Langley intrusion detection systems. The contractor shall provide a method for timely response to suspected intrusions overnight, on weekends and on holidays (and other days that the Center is closed).

The Contractor shall use the Agency standard intrusion detection software, as well as other COTS or Langley-specific tools as directed by the Center ITSM. The Contractor shall review system logs daily for any evidence of unauthorized accesses that were not detected by the intrusion detection software and shall attempt to automate notifications where possible. The intrusion detection systems currently run on a number of Unix and Windows OS-based platforms. Some of these systems run the Agency standard intrusion detection software and others run locally developed or other industry standard software to monitor all traffic entering/leaving the Center. The intrusion detection system shall have a mobile hardware component that can be easily moved from one sub-network to another to monitor traffic during an incident or to support an investigation as directed by the Center ITSM. The Contractor shall report incidents in accordance with the Incident Response work area requirements.

The Contractor shall examine LaRCNET traffic logs for specific systems, as directed by the Center ITSM, to support internal or law enforcement investigations in determining access patterns for inappropriate use or illegal activities.

Work Area Title: Perimeter Protection for LaRCNET

LaRC Manager: Center IT Security

Work Area Description: NASA Langley Research Center - Building 1268 complex and other facilities with connections to LaRCNET as required.

Work Area Requirements: The Contractor shall operate, administer, monitor, and maintain both the hardware and software that comprise the web content filters, the Center Virtual

Private Network (VPN), the Center and Public firewalls, as well as facility-specific firewalls according to NASA and LaRC policy as directed by the Center ITSM.

Authentication to the VPN shall be accomplished using RSA SecurID 60-second token/fobs that generate one-time, non-reusable passcodes. The Contractor shall operate, administer and monitor the RSA ACE authentication servers which provide two-factor authentication to the Center.

Connectivity to the Internet must be re-established in a timely manner in the event of a failure. The Contractor will cooperate with the ODIN Contractor to implement protective measures in the best location, whether that is on the VPN, firewall or on the border routers currently managed by the ODIN Contractor. The Contractor shall not normally implement VPN or firewall policy changes, except in an emergency situation, without first notifying the Center ITSM or his/her designee. In emergencies, the protection of the Center is paramount and the Center ITSM or his/her designee shall be notified as quickly as possible; or no later than 9:00 a.m. the next business day. Based on advisories, bulletins or notification of actual or probable hostile actions against LaRC's IT resources, the Contractor shall make recommendations to the Center ITSM as to possible responses to improve the Center's ITS perimeter.

<u>Work Area Title</u>: System Compliance and Vulnerability Reduction

<u>LaRC Manager</u>: Center IT Security

<u>Work Area Description</u>: NASA Langley Research Center - Building 1268 complex and other facilities with connections to LaRCNET as required.

<u>Work Area Requirements</u>: The Contractor shall operate and maintain both the hardware and software that comprise the LaRC vulnerability scanning system. The Contractor shall utilize the Agency standard vulnerability scanning software to periodically verify that corrective actions have been taken to fix known problems on all systems that are connected to LaRCNET. Other vulnerability scanning software may be used at the direction of the Center ITSM. The Contractor shall conduct vulnerability scans of specific systems at the request of a particular organization or at the direction of the Center ITSM. The Contractor shall operate the vulnerability scanning from designated systems in a fixed location and shall also provide the capability to take the vulnerability scanning out to sub-networks that are behind facility firewalls.

The Contractor shall utilize the patch management system. This includes identifying hosts with known and emerging vulnerability profiles, creating reports at the direction of the Center ITSM, weekly exports of the host lists, weekly deletions or offline hosts, etc.

The Contractor shall perform penetration testing as directed by the Center ITSM or his/her designee.

<u>Work Area Title</u>: Certification and Accreditation (C&A)

<u>LaRC Manager</u>: Center IT Security

<u>Work Area Description</u>: NASA Langley Research Center and nearby Contractor facilities with connections to LaRCNET.

<u>Work Area Requirements</u>: The Contractor shall assist in the development and evaluation of Langley IT System Security Plans and Contingency Plans and report deficiencies or areas requiring clarification to the Center ITSM. The Contractor shall conduct risk analysis in

accordance with NIST specifications and publications for Langley computer systems. The Contractor shall support the risk analysis of and respond to risk assessments, penetration tests or audits conducted by outside organizations, such as the Office of Inspector General. Additionally, the Contractor shall review all security plans and consolidate into fewer plans where it is determined to be appropriate. Also, the Contractor shall evaluate the LaRC C&A Process including any C&A tools sets currently in place. The Contractor shall provide recommendations for addressing any suggested corrective actions.

Work Area Title: VPN & IT Security Helpdesk

LaRC Manager: Center IT Security

Work Area Description: NASA Langley Research Center and nearby Contractor facilities with connections to LaRCNET.

Work Area Requirements: The contractor shall staff a help desk for VPN users, LaRCNET users connecting through the firewall, IT security incidents, and other IT security questions.

Work Area Title: Subtask Reporting of Costs, Actuals, Estimates and Work Completed

LaRC Manager: Center IT Security

Work Area Description: The Contractor shall provide a monthly report to the Center ITSM containing costing information for each subtask worked on under this task.

Work Area Requirements: The costing information shall be provided in an Excel spreadsheet, and mailed to the Center ITSM.

The contents of the spreadsheet shall include but not be limited to the following: A unique work identification tracking number, assigned by TIPS, project title, funding provided (PR), estimated cost (to develop or maintain), actual costs broken down by month, total actual costs, remaining costs (Estimated-Actual) with overruns highlighted, remaining funding PR$s-Actual) with overruns highlighted, and per line item, the contractor shall identify the reasons for cost overruns and provide a revised estimate for completing the project.

Work Area Title: Secondary Public Key Infrastructure (PKI) LaRC Registration Authority (RA)

LaRC Manager: Center IT Security

Work Area Description: NASA Langley Research Center

Work Area Requirements: The contractor shall provide a secondary PKI LaRC RA for emergency recovery during normal business hours.

Work Area Title: Remote Network Access Control (NAC) Evaluation

LaRC Manager: Center IT Security Manager

Work Area Description: Remote access users, via approved virtual private network (VPN) connection, into the LaRC network.

Work Area Requirements: The Contractor shall implement and maintain network access control (NAC) in the LaRC network environment for remote virtual private network (VPN) users. This will be provided using a two-phase approach: first, the Contractor shall evaluate and recommend a NAC product for the LaRC VPN environment; second, based on the Center ITSM approval for the recommended product, proceed with implementation into the production LaRC VPN environment. The contractor shall operate and maintain the NAC product.

Work Area Title: Evaluation and Acquisition of ITS Software and Hardware

LaRC Manager: Langley IT Security

Work Area Description: NASA Langley Research Center - Building 1268 complex and other facilities with connections to LaRCNET as required.

Work Area Requirements: The Contractor shall recommend and evaluate tools and computer systems for use in automating ITS functions, including network traffic analysis, monitoring, intrusion detection, firewalls, virtual private networks, authentication methods, testing and rule or event based countermeasures. The Contractor shall recommend purchases of hardware, software and maintenance to the Langley ITSM. With concurrence of the Langley ITSM, the Contractor shall investigate tools and procedures for alerting appropriate personnel of security incidents on a near-real time basis. The Contractor shall acquire and study tools used to penetrate computer security barriers and develop countermeasures to increase protection. Based on their findings from these tests or emergent conditions in the cyber threat environment, the Contractor shall use an integrated test lab environment to develop implementation or migration plans. New tools will only be implemented into the Langley environment with concurrence of the Langley ITSM.

7. Exhibit A

Exhibit A

8. SPECIAL SECURITY REQUIREMENTS

Personnel assigned to this TA will have privileged access to critical Langley IT resources and require Secret clearances for threat briefings.

9. SOFTWARE ENGINEERING PROCESS REQUIREMENTS

Operations Plan: The contractor shall prepare, keep current, and follow an operations plan for the work areas of this TA, to comply with the operations process and operations plan requirements given in Task Assignment SL001.

10. JOINT REVIEW SCHEDULE

There will be a joint review of the work of this task at meetings to be held weekly in the office of the Center ITSM. The following persons or their alternates are required to attend: Task Manager and Technical Leads leads for this TA in support of the Center ITSM. Technical performance, timeliness, and cost will be discussed.

11. PERIOD OF PERFORMANCE

This TA is effective from 02/01/02 to 04/27/10

12. TECHNICAL PERFORMANCE RATING

In evaluating performance for incident response and computer forensics quality and timeliness shall be rated as follows:

Quality: 25% Timeliness: 75%

In evaluating performance for IT security plans, quality and timeliness shall be rated as follows:

Quality: 50% Timeliness: 50%

In evaluating performance for Coordination of ITS Activities with Other Centers, quality and timeliness shall be rated as follows:

Quality: 75% Timeliness: 25%

In evaluating performance for Intrusion Detection and Monitoring, quality and timeliness shall be rated as follows:

Quality: 25% Timeliness: 75%

In evaluating performance for Perimeter Protection of LaRCNET, quality and timeliness shall be rated as follows:

Quality: 25% Timeliness: 75%

In evaluating performance for scanning LaRCNET, quality and timeliness shall be rated as follows:

Quality: 50% Timeliness: 50%

In evaluating performance for VPN & IT Security Helpdesk, quality and timeliness shall be rated as follows:

Quality: 50% Timeliness: 50%

13. RESPONSE REQUIREMENTS

The Task Plan shall address the contractor's lead personnel; specific work plans; and the associated estimated labor hours, cost, and schedule.

14. FUNDING INFORMATION

Funding has not been entered for this TA.

15. MILESTONES

None required.

16. DELIVERABLES

Number	Deliverable Item	Deliverable Schedule
1	Incident Response Reports	The Contractor shall prepare a report of the impact of each incident to include costs due to loss of data; time lost due to the unavailability of the system; time to rebuild the system; time to investigate the incident and any other factors with a cost implication. The reports shall also include findings on the

		method of intrusion and corrective actions taken to reduce the system's vulnerability. This report is due one week after the system is returned to service.
2	Risk Analysis	The Contractor shall prepare a report documenting the findings of a risk analysis within sixty days of the scheduled start of the analysis, unless otherwise agreed to by the customer or the Center ITSM. The system owner shall be briefed within one week, or at the owner's earliest convenience, on all findings at the completion of the analysis. Copies of the report shall be available to the system owner and Center ITSM no later than this briefing.
3	Quarterly ITS Metrics	The Contractor shall prepare a quarterly report on ITS metrics, as defined by the NASA Competency Center for IT Security no later than the 5th day of each quarter (or next business day after the 5th). These reports are due on January 5th, April 5th, July 5th and October 5th respectively.
4	Monthly ITS Status Report	The Contractor shall provide the Center ITSM with a status report (encrypted e-mail is acceptable) by the fifth business day of each month on the firewall, virtual private network, intrusion detection system, incident response procedures, vulnerability scanning and reduction procedures or other significant ITS activities.
5	Certification & Accreditation (C&A) Process	The Contractor shall provide the Center ITSM with an evaluation of LaRC C&A process by September 30, 2009.
6	Security Plan Consolidation	The Contractor shall provide the Center ITSM with a recommendation for consolidating LaRC Security Plans where appropriate by October 15, 2009.

17. FILE ATTACHMENTS

None.